UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/509,872	02/03/2005	Hideyuki Suzuki	259551US6PCT	4966

22850 7590 10/13/2010

OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, L.L.P.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
ARMOUCHE, HADI S	

ART UNIT	PAPER NUMBER
2432	

NOTIFICATION DATE	DELIVERY MODE
10/13/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

Office Action Summary	Application No.	Applicant(s)	
	10/509,872	SUZUKI, HIDEYUKI	
	Examiner	Art Unit	
	HADI ARMOUCHE	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 July 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) *6,8,9,12-14 and 16-18* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,7,10,11 and 15* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This communication is in response to applicant's amendment filed on 07/22/2010. Claims 4, 7 and 15 have been amended; claims 6, 8-9, 12-14 and 16-18 have been withdrawn; claims 1-18 remain pending.

2. Applicant's election without traverse of group 1 (claims 1-5, 7, 10, 11 and 15) in the reply filed on 01/07/2010 is acknowledged.

Response to Arguments

3. Applicant's arguments with respect to claims 1-5, 7, 10, 11 and 15 have been considered but are moot in view of the new ground(s) of rejection.

4. Applicant's arguments (page 12 of the remarks) regarding the 35 U.S.C 112, second paragraph rejection are persuasive. Rejection to claims 2-5, 7 and 10 under 35 U.S.C. 112, second paragraph is hereby withdrawn.

5. Applicant's arguments (page 13 of the remarks) regarding the 35 U.S.C 101, rejection are persuasive. Rejection to 4, 5, 7 and 10 under 35 U.S.C.101 is hereby withdrawn.

6. Applicant's amendment to claim 15 obviates previously raised claim rejection under 35 U.S.C 101. Rejection to claim 15 under 35 U.S.C 101 is hereby withdrawn.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1-3 are rejected under 35 U.S.C. 103(a) as being unpatentable over Doe et al. (US 6,496,928) referred to hereinafter by Doe in view of Kadansky et al. (US 6,295,361) referred to hereinafter by Kadansky.

9. Regarding claim 1, Doe teaches *a wireless ad-hoc communication system including a plurality of terminals, the communication system comprising:*

a first terminal configured to encrypt a payload of a broadcast frame and to transmit the broadcast frame [Figure 1 element 12, col 22 lines 15-25 and col 26 lines 7-10]*;*

a second terminal configured to receive the broadcast frame and to decode the payload of the broadcast frame [Figure 1 element 18 and col 22 lines 15-25]*, wherein*

the first terminal is configured to encrypt the payload of the broadcast frame using a broadcast encryption key assigned to the first terminal [col 22 lines 15-45 and col 26 lines 7-10]]*;*

the second terminal is configured to determine an end-terminal identifier (address) *in the broadcast frame as a broadcast address, and decode the payload of the broadcast frame using the broadcast encryption key assigned to the first terminal* [col 22 lines 26-45, col 27 lines 1-19 and col 27 line 42-col 28 line 31].

Doe doesn't explicitly disclose that *any terminal in the plurality of terminals is configured to perform the role of said first terminal and said second terminal.* However,

Kadansky discloses any terminal in the plurality of terminals may perform the role of said first terminal or said second terminal (see fig. 1, and "A node may be both a sender and a receiver of data to and from other nodes, col. 1, lines 29-31). It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify Doe with Kadansky to enable first and second terminals have interchangeable role and this allow a terminal to transmit and receive data to and from other terminals.

10. Regarding claim 2, Doe teaches that *the second terminal includes: an encryption-key management list table having at least an encryption-key management list including a set of a terminal identifier of the first terminal and the broadcast encryption key assigned to the first terminal; means for searching the encryption-key management list table based on the terminal identifier of the first terminal included in an origination-terminal identifier of the received broadcast frame to extract the corresponding broadcast encryption key assigned to the first terminal; and means for decoding the payload of the broadcast frame using the extracted broadcast encryption key assigned to the first terminal* [col 22 lines 15-45, col 27 line 12-col 28 line 31].

11. Regarding claim 3, Doe teaches that *wherein the first terminal includes: a generated-key table configured to store the broadcast encryption key assigned to the first terminal; means for encrypting the payload of the broadcast frame using the broadcast encryption key assigned to the first terminal stored in the generated-key table; and means for transmitting the encrypted broadcast frame* [col 22 lines 15-45, col 26 lines 7-23 and col 27 line 12-col 28 line 31].

12. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Stallings, "Cryptography and Network Security: Principles and Practice", 3rd edition, Pearson Education, pages 388-389.

13. Regarding claim 10, Stallings teaches *a terminal comprising:*

means for receiving a terminal identifier and other data *of a different terminal from the different terminal* [step 1 of Public-Key Encryption Approaches, end of page 388 wherein A (different terminal) sends AS (receiving terminal) A's ID and other data (B's ID)]*;*

means for encrypting the terminal identifier and the other data *of the different terminal using a broadcast encryption key assigned to the terminal* [step 2 of Public-Key Encryption Approaches, end of page 388 wherein AS (receiving terminal) encrypts A's ID and the other data with KR_{as}]*; and*

means for broadcasting the encrypted terminal identifier and other data of the different terminal [step 2 of Public-Key Encryption Approaches, end of page 388 wherein AS sends/broadcast the encrypted data to A].

However, Stallings' authentication protocol on page 388 does not explicitly teach that the "other data" of the different terminal (A) is A's *broadcast encryption key.* Stallings' authentication protocol on page 389 step 2 shows that the KDC is encrypting B's ID and B's key using KR_{auth} key.

At the time of the invention was made, it would have been obvious to an ordinary skill in the art to modify Stallings' authentication protocol on page 388 to indicate that

the other data is a key as taught by Stallings' authentication protocol on page 389. The motivation/suggestion would have been to allow any receiving terminal (other than A, AS and KDC) to communicate with the terminal B using B's key.

Claim Rejections - 35 USC § 102

14. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

15. Claims 4-5, 7, 11 and 15 are rejected under 35 U.S.C. 102(b) as being anticipated by Doe et al. (US 6,496,928) referred to hereinafter by Doe.

16. Regarding claim 4, Doe teaches *a terminal comprising:*

an encryption-key management list table having at least one encryption-key management list comprising a terminal identifier of a different terminal, a unicast encryption key between the terminal and the different terminal, and a broadcast encryption key assigned to the different terminal [col 23 line 19-col 24 line 17, col 22 lines 15-45 and col 27 line 12-col 28 line 31];

means for searching the encryption-key management list table for the encryption-key management list including an origination-terminal identifier of a corresponding to an originating terminal identifier in a received broadcast frame [col 27 line 12-col 28 line 31];

means for extracting a broadcast encryption key from the encryption-key management list that corresponds to the origination-terminal [col 27 line 12-col 28 line 31]*; and*

means for decoding a payload of the broadcast frame using the extracted broadcast encryption key [col 28 lines 20-31].

17. Regarding claim 5, Doe teaches *a terminal comprising:*

an encryption-key management list table having at least one encryption-key management list configured to store a unicast encryption key between said terminal and a different terminal and a broadcast encryption key assigned to the different terminal in association with a terminal identifier of the different terminal [col 23 line 19-col 24 line 17, col 22 lines 15-45 and col 27 line 12-col 28 line 31];

means for searching, when a destination-terminal identifier of a received frame is a broadcast address, the encryption-key management list table for the encryption-key management list including an origination-terminal identifier of the frame to extract the corresponding broadcast encryption key as an encryption key, and when the destination- terminal identifier of the received frame is other than a broadcast address, searching the encryption-key management list table for the encryption-key management list including an origination-terminal identifier of the frame to extract the corresponding unicast encryption key as the encryption key [col 27 line 12-col 28 line 31]*; and*

means for decoding a payload of the frame using the extracted encryption key [col 28 lines 20-31].

18. Regarding claim 7, Doe teaches *a terminal comprising:*

a generated-key table configured to store a broadcast encryption key assigned to said terminal [col 23 line 19-col 24 line 17, col 22 lines 15-45 and col 27 line 12-col 28 line 31];

an encryption-key management list table having at least one encryption-key management list configured to store a unicast encryption key between said terminal and a different terminal in association with a terminal identifier of the different terminal [col 23 line 19-col 24 line 17, col 22 lines 15-45 and col 27 line 12-col 28 line 31];

means for, when a frame to be transmitted is a broadcast frame indicated by an end-terminal identifier being a broadcast address, encrypting a payload of the broadcast frame using the broadcast encryption key of the generated-key table, and when the frame to be transmitted is a unicast frame indicated by an end-terminal identifier not being a broadcast address, searching the encryption-key management list table for the encryption-key management list including a destination-terminal identifier of the unicast frame to encrypt a payload of the unicast frame using the corresponding unicast encryption key; and means for transmitting the encrypted frame [col 27 line 12-col 28 line 31]*;*

19. Regarding claims 11 and 15, Doe teaches *a method for decoding a broadcast frame in a terminal that includes an encryption-key management list table having at least one encryption-key management list including a terminal identifier of a different terminal, a unicast encryption key assigned for communication between the terminal and the different terminal, and a broadcast encryption key assigned to the different*

terminal [col 23 line 19-col 24 line 17, col 22 lines 15-45 and col 27 line 12-col 28 line 31] *the method comprising:*

searching the encryption-key management list table for the encryption-key management list including an origination-terminal identifier corresponding to an originating terminal identifier in a received broadcast frame to extract a broadcast encryption key corresponding to the origination-terminal identifier [col 27 line 12-col 28 line 31]*; and*

decoding a payload of the broadcast frame using the extracted broadcast encryption key [col 28 lines 20-31].

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to HADI ARMOUCHE whose telephone number is (571)270-3618. The examiner can normally be reached on M-Th 7:30-5:00 and Fridays half day.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/H. A./
HADI ARMOUCHE
Examiner, Art Unit 2432

/Benjamin E Lanier/
Primary Examiner, Art Unit 2432